

Coalition for Open Digital Ecosystems

Comments on the DMA Evaluation Public Consultation

1. Introduction

This submission is made by the Coalition for Open Digital Ecosystems (“**CODE**”)¹ in the context of the public consultation by the European Commission (the “**Commission**”) on the first review of the Digital Markets Act (“**DMA**”).²

CODE brings together companies sharing a commitment to four core principles, namely: (i) opening up digital ecosystems through cross-industry collaboration; (ii) promoting seamless connectivity and interoperable systems to fuel innovation; (iii) empowering consumers to choose devices and services with ease; and (iv) nurturing an environment of open access. CODE members share the conviction that open digital ecosystems are better for businesses, consumers and society. CODE has a strong interest in the DMA achieving its aims of contestability and fairness in digital markets and fully supports the Commission’s aim to ensure effective enforcement of the interoperability obligations.

CODE is committed to making a meaningful contribution to the pursuance of openness and interoperability by working together with industry players, civil society and public bodies to exchange ideas, encourage and promote research, and support open standards and interoperability. It is in this context that CODE offers the below comments on the Commission’s public consultation concerning the evaluation of the DMA.

2. The list of core platform services and designated services

CODE does not deem necessary, at this stage, to include new core platform services (“**CPSS**”) or to expand the list of obligations imposed on gatekeepers and gatekeeper services. This conversation, if at all, should take place once effective compliance with the existing obligations in respect of existing CPS categories is secured. In particular, in CODE’s view, it is not warranted to expand the list of CPS categories and obligations until effective interoperability is implemented as standard for designated platforms.³ Article 6(7) of the DMA is already a powerful tool for addressing existing and emerging bottlenecks within operating systems (“**OSs**”) and is already broad enough to cover software as well as hardware features.

¹ CODE’s membership includes various tech companies of very different sizes, activities, origins and business models. See <https://www.opendigitalecosystems.org/>. CODE members are Flywallet, Garmin, Google, Honor, Lenovo, Lynx, Meta, Motorola, Nothing, Opera, Qualcomm, Vodafone and Wire. CODE is an open coalition and any company that subscribes to CODE’s core principles is welcome to join.

² See European Commission’s public consultation launched on 3 July 2025 on the first review of the DMA, available [here](#).

³ See Decision of 19 March 2025 in case DMA.100204, *Process*, para. 104, where the Commission confirms that, under Article 6(7) DMA, Apple is required to ensure that the relevant features are effectively interoperable and that compliance should be by design and free of charge. The Commission adds that “*such a proactive approach to compliance and interoperability by design should be adopted by default with respect to new features, released after the adoption of the Specification Decision*”.

As concerns artificial intelligence (“**AI**”) specifically, CODE agrees that the DMA should be equipped to address AI-related issues as and when they emerge. However, in CODE’s view, it is not necessary or indeed useful to create new AI-related CPS categories. AI is a foundational technology, not a product that can be encapsulated into a predefined CPS category. Indeed, AI technology is already part of, and covered by, various existing CPS categories (e.g., OSs, web browsers, virtual assistants (“**VAs**”)). As things stand, CODE considers that the DMA and its CPS categories already adequately cover AI and AI-based technologies, including CPS categories in which AI is likely to play an increasingly important role.

Today, as a general matter, the AI space in the EU is highly competitive and dynamic, and if Europe is to make the most of the “AI revolution” for both businesses and citizens, the Commission should encourage and support the development, distribution, growth and adoption of innovative AI technologies, without engaging in overregulation that may stifle this nascent and highly promising sector. At the same time, CODE encourages the Commission to closely monitor AI-related technologies and products and use the DMA and other appropriate tools to address issues if and when they arise.

For instance, while the application of the DMA to VAs remains untested, the Commission should ensure that users have the freedom to download, select and easily switch their preferred AI assistant as the default, and that OEMs can partner with a diverse range of AI assistants to deliver an attractive experience for users. AI assistants should be able to access the relevant features and functionalities provided by the OS and available to the OS provider’s own products and services, while taking account of requirements such as memory, battery life, security, etc..

Beyond AI, CODE encourages the Commission to revisit and reverse its decision not to designate iMessage, Apple’s number-independent interpersonal communications services (“**N-IICSs**”). The Commission has already concluded that Apple’s iMessage is a N-IICS that meets the quantitative thresholds of Article 3(2) DMA.⁴ An “exceptional” derogation from designation is not warranted. iMessage is the only messaging service that allows business users to reach 100% of Apple’s hundreds of millions of premium end users. No other communication service can replicate or match this advantage.

Designating iMessage is key to enabling consumers and business users to seamlessly communicate with each other across different services and ecosystems and would decrease switching costs, prevent lock-in, and level the playing field for messaging services. Despite the Commission’s conclusion that iMessage lacked widespread usage, it remains a CPS, which reinforces Apple’s lock-in of users into its wider ecosystem. In addition, the non-designation of iMessage has resulted in the incongruous situation that the only N-IICSs

⁴ See Commission Decision of 5 September 2023 in Cases DMA.100013 *Apple – online intermediation services – app stores*, DMA.100025 *Apple – operating systems* and DMA.100027 *Apple – web browsers*, para 159. Apple has challenged before the EU General Court the Commission’s conclusion that iMessage is a N-IICS (Cases T-1079/23 *Apple v Commission* and T-1080/23 *Apple v Commission*). CODE strongly supports the Commission’s conclusion that iMessage is an N-IICS and urges the General Court to dismiss Apple’s applications on this issue.

designated under the DMA, and thus subject to the interoperability requirements of Article 7 DMA, are WhatsApp and Messenger, which both belong to the same undertaking, Meta. In addition, the one messaging app that sits within a closed ecosystem is not designated, whereas WhatsApp and Messenger are cross-platform.

To further these goals, the Commission should also keep monitoring Apple's implementation of the Rich Communication Services ("RCS") protocol on iOS, which does not yet allow users to send end-to-end encrypted RCS messages and in-line replies, edit messages, and unsend messages across platforms and services that support RCS. Apple should also support future RCS improvements where relevant to further the goals of the DMA. These changes would offer users a much-improved experience when communicating across platforms.

When considering possible additional gatekeeper CPS designations, CODE encourages the Commission to focus on enabling interoperability and freeing users from ecosystem lock-in, both of which are crucial to opening up closed "walled garden" digital ecosystems and achieving the DMA's dual goals of promoting contestability and fairness in digital markets. For these reasons, CODE encourages the Commission to consider the designation of Apple CPSs such as FaceTime, which is an extension of iMessage, and iCloud, which increasingly stores users' data. Both of which are significant sources of gatekeeper power and lock-in within Apple's digital ecosystem. FaceTime represents the only native video calling solution on iPhones, which causes accessibility issues. If FaceTime were designated as a CPS, it would allow competing video call services to have equal access to iOS, providing a much-needed out-of-the-box solution for users with accessibility needs.

3. The importance of securing true interoperability and open access

In CODE's view, interoperability by design as mandated by Article 6(7) DMA is one of the core principles of the DMA.

Interoperability is key to promoting innovation, diversity, choice, fairness and contestability. CODE firmly believes that consumers should be free to choose the products and services that best suit their needs and preferences, free from any constraints imposed by the OS the devices connect with, and to switch between different OSs without foregoing the benefits of the connected physical devices they have already acquired or would want to acquire.

Effective interoperability means equally effective interoperability. Third parties should benefit from solutions that are as equally effective as those provided for the gatekeeper's own features and services and should not be impeded in their use of the underlying CPS to reach and interact with their own consumers. Developers should be enabled to deliver consistent functionality across ecosystems, without degraded performance or artificial restrictions. This is only possible if third parties receive non-discriminatory and effective interoperability with, and access to, for the purposes of interoperability, OS software and device capabilities available to the firm that controls them.

Open access to OS software and hardware features is critical for EU businesses, developers, manufacturers and entrepreneurs to innovate and compete. When platforms grant equal and

unfettered access to OS APIs and device capabilities, they lower entry barriers and foster a diverse, competitive market. It also supports repairability and upcycling, and extends the useful life of hardware, contributing to broader sustainability goals.

Interoperability is also critical for EU consumers. There is strong consumer demand for seamless, secure interoperability. Consumers today increasingly demand transparency, portability, and control over their device choices. According to CODE's consumer survey carried out in February 2025,⁵ over 80% of respondents stated that interoperability is important to them, and over 90% agree that smartphone companies should ensure their devices work equally well with products from other brands.

CODE welcomes the efforts made by the Commission in this regard. The Commission rightly identified the risks of undermining the objectives of the DMA posed by closed ecosystems and acted promptly to tackle these practices. In this sense, EU businesses and end users will benefit from the Commission's specification decisions⁶ setting down how Apple must allow for effective interoperability with its OS, both procedurally and substantively, in respect of connected devices. While we are pleased that Apple *announced* plans to implement certain features as mandated by the Commission's specification decision, these benefits will only materialise if the specification measures are effectively implemented by Apple and these important features are made available in an effective manner. We also encourage the Commission to monitor the effectiveness of its specification decision, such as whether the requirements relevant to Airdrop provide for effective alternatives for consumers to engage in critical data sharing use cases across platforms.

Despite these initial positive developments, further work remains to be done. The goal is and should remain interoperability by design. CODE encourages the Commission not to settle for less.

4. CODE's recommendations for future DMA Enforcement

Overall, CODE believes that DMA enforcement by the Commission should be guided by the key principles of transparency, predictability and fairness. On that basis, CODE has identified the following aspects that would require closer attention:

a. Asymmetry of the efforts to comply with the DMA

CODE understands that the Commission is interested in hearing market views on the quality and means through which gatekeepers are demonstrating compliance with their obligations under the DMA.

We understand that the DMA is a novel legal tool creating many new rights and obligations and thus there remains a degree of uncertainty. To that end, exercises such as the workshops organised by the Commission may prove a useful tool to gain a deeper understanding of the

⁵ See Polling Europe Survey on perceptions on hardware interoperability of February 2025, available [here](#).

⁶ Decision of 19 March 2025 in case DMA.100203, *Connected Physical Devices*, and Decision of 19 April 2025 in case DMA.100204, *Process* (the "**Specification Decisions**").

compliance measures put in place by gatekeepers and how those measures impact third parties, as well as fostering regulatory dialogue between the gatekeeper and the Commission, but effective compliance with Article 6(7) DMA will at times entail a degree of technical precision that requires additional transparency and accountability (e.g., publication of more detailed plans relating to implementation, and in a timely manner).

In CODE's experience, Apple's implementation of the Commission's Specification Decisions under Article 6(7) has lacked transparency. To date, Apple's DMA efforts have at times appeared to be more focused on diluting or evading its legal obligations than complying with them in good faith and reveal a fundamental misalignment in the understanding of interoperability both in terms of process and substance. Since its entry into force, Apple has systematically tried to diminish the effectiveness of the DMA by creating an uncertain and artificially complex environment for app developers,⁷ making contentious and provocative public statements⁸ and scaring end users with inaccurate privacy and security claims.⁹ Apple has tried at every turn to obfuscate, delay, and put in place half-measures,¹⁰ "benefitting" all the while from its non-compliance.¹¹

The ultimate objective of Apple's obstructionist strategy is to maintain the pre-DMA *status quo* and delay as long as possible the transition from "walled garden" to openness and effective interoperability. Contrary to this, compliance with Article 6(7) DMA should be proactive and an inherent part of Apple's design decisions.¹²

⁷ See Decision of 19 March 2025 in case DMA.100204, paras. 105-106 and 141 where the Commission explains that Apple's request-based approach to interoperability limits developers' rights by unreasonably and impractically shifting the burden of identifying interoperability gaps onto them, which in the absence of sufficient transparency would make it difficult or impossible for developers to understand what the reserved features are and what capabilities they provide. See also para. 150 and accompanying footnote 184 of that Decision, where the Commission asks Apple to provide more transparency in light of the difficulties that developers themselves have raised in this regard.

⁸ See 2nd DMA enforcement workshop: Apple - Update on first year of DMA compliance, 30 June 2025, available at: <https://webcast.ec.europa.eu/2nd-dma-enforcement-workshop-apple-update-on-first-year-of-dma-compliance-2025-06-30>. Apple representatives stated, *inter alia*, that: "Some third parties are weaponising interoperability to access users' personal information" and that "Providing third parties with unfettered access to every part of every EU user's iPhone, like these requests would have us do, would compromise user privacy and security, and it is contrary to what was set out in the GDPR. The DMA was explicitly intended to not undermine the GDPR yet it seems we are constantly being asked to do just that".

⁹ See, for instance, Decision of 23 April 2025 in DMA.100109, e.g., at paras. 63, 79 and 113-116, where the Commission states that Apple cannot raise a "security" exception in relation to Article 5(4) DMA and does not substantiate the security concerns it makes.

¹⁰ See, for instance, Decision of 23 April 2025 in DMA.100109, at paras. 47-52, where, with regard to compliance with Article 5(4) DMA, the Commission explicitly rejects Apple's approach of offering multiple sets of business terms – i.e., one that complies with Article 5(4) DMA and others that do not – as a DMA compliance strategy.

¹¹ See 2nd DMA enforcement workshop: Apple - Update on first year of DMA compliance, 30 June 2025, available at: <https://webcast.ec.europa.eu/2nd-dma-enforcement-workshop-apple-update-on-first-year-of-dma-compliance-2025-06-30>. Apple representatives sought to justify its behaviour by stating, "You all know how much Apple users value the privacy and security of their data. That's one of the many reasons they choose Apple over our competitors' products and why we work so hard to keep their data safe. If we are forced to give up that value, this places our users at risk while compromising what makes Apple unique". Of course the real value for Apple is its use of privacy, safety and integrity to justify belated and reluctant compliance, all the while continuing to reap the benefits of its closed ecosystem.

¹² See Decision of 19 March 2025 in case DMA.100204, para. 54.

Both the Commission and stakeholders have characterised Apple’s measures to comply with Article 6(7) DMA as being excessively complex, reactive and intransparent.¹³ The publicly accessible version of Apple’s first DMA compliance report was a mere 12 pages long (just one and a half of which was on “*interoperability in the EU*”).¹⁴ This is clearly insufficient. Although the second DMA compliance report was more extensive, its length did not resolve the complexity and shortcomings. While ostensibly clear, Apple’s implementation of the interoperability request process has, in practice, artificially created and maintained an unclear framework for developers, the effect of which has been to diminish the effectiveness of the DMA. The interoperability request form published by Apple is also manifestly insufficient in terms of the levels of information and transparency afforded to third parties with respect to features of the operating system and the levels of responsiveness and tailoring of specific interoperability solutions for third parties. Apple’s bureaucratic process is a feature of their closed model, not a bug. As a result, thousands of EU developer hours are wasted on Apple’s request form, contrasted with the zero hours required to access public, documented APIs in an open operating system.

Apple’s disobliging attitude was further demonstrated in the workshop held on 30 June 2025, where Apple made incorrect claims that for it to comply with its obligations under Article 6(7) DMA would cause risks for users, creating roadblocks for both Apple’s and developers’ software engineering and forcing Apple to delay the rollout of new features in the EU.¹⁵ In the same workshop, Apple spuriously claimed that the interoperability requirements of the DMA are being applied unfairly towards Apple, whereas the reality is that Apple is finally being obliged to open up its closed ecosystem to the benefit of consumers and developers, as other market players have done for years. If Apple is required to go to further lengths than other gatekeepers to comply with Article 6(7) DMA, that is merely reflective of the fact that Apple’s “walled garden” model was very far from effective compliance. CODE therefore urges the Commission to closely monitor that Apple effectively complies with the Specification Decisions in cases DMA.100203 and DMA.100204, and that Apple takes the appropriate steps to ensure interoperability by design, the ultimate goal of the DMA.

This is a clear goal that leaves no room for interpretation. In the absence of Apple moving towards an open-source OS, which is inherently interoperable, all major new Apple features must be interoperable from day one. Should Apple not comply with the Specification Decisions, belatedly put measures in place or not make future features interoperable by design, CODE encourages the Commission to act swiftly, especially in situations where noncompliance by Apple with the Specification Decisions would be obvious. A lengthy procedure, which would relate to legal obligations that have applied to Apple since March

¹³ See Decision of 19 March 2025 in case DMA.100204, e.g., at paras. 105-108, where the Commission criticises Apple’s burdensome, intransparent and complex request-based approach that risks delays and leaving Apple in control; see also footnote 138 of para. 106, citing criticisms from respondents to the Commission’s public consultation.

¹⁴ See Apple’s first DMA compliance report of 1 November 2024, available [here](#), pages 7 and 8.

¹⁵ See 2nd DMA enforcement workshop: Apple - Update on first year of DMA compliance, 30 June 2025, available at: <https://webcast.ec.europa.eu/2nd-dma-enforcement-workshop-apple-update-on-first-year-of-dma-compliance-2025-06-30>.

2024, only benefits Apple at the expense of EU developers and consumers. CODE trusts that the Commission will take all the necessary steps to ensure that such undesirable outcomes are avoided.

b. The exceptions invoked to hinder interoperability should be proportionate and narrowly drawn

The DMA, and notably Article 6(7), allow gatekeepers to put in place measures whose objective is to protect system integrity. However, Apple has misused (and misinterpreted)¹⁶ this exception, weaponising it in an effort to maintain its “walled garden”.

Apple has systematically made public claims and devoted a significant portion of its DMA compliance workshop on 30 June 2025 to raising privacy and security concerns. Apple also invoked unsubstantiated claims of how complying with its interoperability obligations under the DMA would jeopardise its intellectual property rights (“IPRs”)¹⁷ (see **section c** below). Leaving aside the fact that none of these considerations would justify a restriction to effective interoperability, CODE agrees with the Commission that it is not legitimate for Apple to impose its own model of security and privacy on third-party devices.¹⁸

Unlocking consumer and developer choice through interoperability and the freedom to choose preferred apps and services will reduce entry barriers, support homegrown talent, boost productivity across sectors, and drive digital competition. Contrary to what Apple claims, this does not necessarily come at a cost to user privacy or the security and integrity of systems, both of which can be protected through proportionate and justified protective measures. Interoperability for developers can co-exist with user privacy through the use of user consent and app-purpose-specific system permissions. Similarly, true security should not depend on secrecy but on the robustness of the security mechanisms themselves.

Therefore, the Commission should be vigilant concerning gatekeepers that seek to rely on integrity concerns as a means to block interoperability. Restrictions based on these interests must be necessary and proportionate, with the onus on the party invoking these interests to show that they are justified.¹⁹ **Any potential integrity restrictions must be proportionate (i.e., strictly necessary and justified) and evidence-based.**²⁰

c. Interoperability is compatible with the respect of IPRs

¹⁶ As the Commission has explained to Apple, only safeguarding integrity could justify the adoption of constructive and proportionate measures under Article 6(7) DMA. Integrity is defined as a property of a feature or service (see, e.g., Decision in Case DMA.100204, para. 83). Therefore, the concepts of privacy and security are alien to Article 6(7) DMA.

¹⁷ Decision in case DMA.100204, paras. 132, 135 and 136.

¹⁸ Decision in Case DMA.100203, para. 107.

¹⁹ Other authorities have already rejected as disproportionate Apple’s privacy arguments when they were used to justify creating artificially complex user consent journeys, to the benefit of Apple’s own services (see Decision of the French Competition Authority of 31 March 2025, available [here](#), particularly paras. 521-541 and 622).

²⁰ See Recital 50 and Article 6(7) DMA.

As explained above, security and integrity concerns are not a justification for closed systems or customer lock-in. Indeed, the notion that open systems are inherently less secure than their closed counterparts is a common misconception, based on the flawed principle that closed systems are always more secure simply because their inner workings are hidden. Apple has chosen to maintain closed proprietary protocols when there are perfectly secure and widely used industry-wide standards, such as Wi-Fi Aware, or RCS, which Apple only belatedly adopted after complaints from users and industry stakeholders. Using this choice in its favour, Apple seeks to invoke respect for IPRs as an excuse to avoid supporting interoperability.

Although it appears that Apple has never publicly invoked specific arguments to justify how or why its IPRs and trade secrets would be jeopardised by the DMA, Apple's decision not to follow open, secure and widely-adopted industry standards when available but use its non-standardised proprietary protocols voids this line of argument. Open standards can and do function in full compliance with IPRs.

Moreover, secure, agreed and workable interoperability standards promote integrity and security. CODE thus invites the Commission to take into account the existence and accessibility of any relevant open and public industry standard when assessing the means, effort and appropriateness of the timelines put forward by Apple to effectively comply with Article 6(7) DMA.

5. Conclusion

CODE respectfully asks that the Commission consider these positions and trusts that it will take all the necessary steps to ensure that EU developers and manufacturers benefit from open access and interoperability, thereby ensuring fair and contestable markets, to the ultimate benefit of EU consumers.

CODE is grateful for the Commission's attention and consideration of these important issues and stands ready to assist the Commission in respect of any of these – or other – issues in the context of the evaluation process.